CertNexus

Exam Questions CFR-410

CyberSec First Responder (CFR) Exam

NEW QUESTION 1
A company website was hacked via the following SQL query: email, passwd, login_id, full_name FROM members WHERE email = “attacker@somewhere.com”; DROP TABLE members; –” Which of the following did the hackers perform?

A. Cleared tracks of attacker@somewhere.com entries
B. Deleted the entire members table
C. Deleted the email password and login details
D. Performed a cross-site scripting (XSS) attack

Answer: C

NEW QUESTION 2
After a hacker obtained a shell on a Linux box, the hacker then sends the exfiltrated data via Domain Name System (DNS). This is an example of which type of data exfiltration?

A. Covert channels
B. File sharing services
C. Steganography
D. Rogue service

Answer: A

NEW QUESTION 3
A network security analyst has noticed a flood of Simple Mail Transfer Protocol (SMTP) traffic to internal clients. SMTP traffic should only be allowed to email servers. Which of the following commands would stop this attack? (Choose two.)

A. iptables -A INPUT -p tcp –dport 25 -d x.x.x.x -j ACCEPT
B. iptables -A INPUT -p tcp –sport 25 -d x.x.x.x -j ACCEPT
C. iptables -A INPUT -p tcp –dport 25 -j DROP
D. iptables -A INPUT -p tcp –destination-port 21 -j DROP
E. iptables -A FORWARD -p tcp –dport 6881:6889 -j DROP

Answer: AC

NEW QUESTION 4
An administrator investigating intermittent network communication problems has identified an excessive amount of traffic from an external-facing host to an unknown location on the Internet. Which of the following
BEST describes what is occurring?

A. The network is experiencing a denial of service (DoS) attack.
B. A malicious user is exporting sensitive data.
C. Rogue hardware has been installed.
D. An administrator has misconfigured a web proxy.

Answer: B

NEW QUESTION 5
While planning a vulnerability assessment on a computer network, which of the following is essential? (Choose two.)

A. Identifying exposures
B. Identifying critical assets
C. Establishing scope
D. Running scanning tools
E. Installing antivirus software

Answer: AC

NEW QUESTION 6
A common formula used to calculate risk is:+ Threats + Vulnerabilities = Risk. Which of the following represents the missing factor in this formula?

A. Exploits
B. Security
C. Asset
D. Probability

Answer: C

NEW QUESTION 7
Detailed step-by-step instructions to follow during a security incident are considered:

A. Policies
B. Guidelines
C. Procedures
D. Standards

Answer: C

NEW QUESTION 8
A Linux administrator is trying to determine the character count on many log files. Which of the following command and flag combinations should the administrator use?

A. tr -d
B. uniq -c
C. wc -m
D. grep -c

Answer: C

NEW QUESTION 9
An administrator believes that a system on VLAN 12 is Address Resolution Protocol (ARP) poisoning clients on the network. The administrator attaches a system to VLAN 12 and uses Wireshark to capture traffic. After reviewing the capture file, the administrator finds no evidence of ARP poisoning. Which of the following actions should the administrator take next?

A. Clear the ARP cache on their system.
B. Enable port mirroring on the switch.
C. Filter Wireshark to only show ARP traffic.
D. Configure the network adapter to promiscuous mode.

Answer: D

NEW QUESTION 10
While reviewing some audit logs, an analyst has identified consistent modifications to the sshd_config file for an organization's server. The analyst would like to investigate and compare contents of the current file with archived versions of files that are saved weekly. Which of the following tools will be MOST effective during the investigation?

A. cat * | cut –d ',' –f 2,5,7
B. more * | grep
C. diff
D. sort *

Answer: C

NEW QUESTION 10
A first responder notices a file with a large amount of clipboard information stored in it. Which part of the MITRE ATT&CK matrix has the responder discovered?

A. Collection
B. Discovery
C. Lateral movement
D. Exfiltration

Answer: D

NEW QUESTION 11
During the forensic analysis of a compromised computer image, the investigator found that critical files are missing, caches have been cleared, and the history and event log files are empty. According to this scenario, which of the following techniques is the suspect using?

A. System hardening techniques
B. System optimization techniques
C. Defragmentation techniques
D. Anti-forensic techniques

Answer: D

NEW QUESTION 13
A government organization responsible for critical infrastructure is being attacked and files on the server been deleted. Which of the following are the most immediate communications that should be made regarding the incident? (Choose two.)

A. Notifying law enforcement
B. Notifying the media
C. Notifying a national compute emergency response team (CERT) or cybersecurity incident response team (CSIRT)
D. Notifying the relevant vendor
E. Notifying a mitigation expert

Answer: CE

NEW QUESTION 17
A user receives an email about an unfamiliar bank transaction, which includes a link. When clicked, the link redirects the user to a web page that looks exactly like their bank's website and asks them to log in with their username and password. Which type of attack is this?

A. Whaling

B. Smishing
C. Vishing
D. Phishing

Answer: D

NEW QUESTION 20
Which of the following describes United States federal government cybersecurity policies and guidelines?

A. NIST
B. ANSI
C. NERC
D. GDPR

Answer: A

NEW QUESTION 23
An incident handler is assigned to initiate an incident response for a complex network that has been affected by malware. Which of the following actions should be taken FIRST?

A. Make an incident response plan.
B. Prepare incident response tools.
C. Isolate devices from the network.
D. Capture network traffic for analysis.

Answer: D

NEW QUESTION 26
An attacker intercepts a hash and compares it to pre-computed hashes to crack a password. Which of the following methods has been used?

A. Password sniffing
B. Brute force attack
C. Rainbow tables
D. Dictionary attack

Answer: C

NEW QUESTION 27
A security administrator is investigating a compromised host. Which of the following commands could the investigator use to display executing processes in real time?

A. ps
B. top
C. nice
D. pstree

Answer: B

NEW QUESTION 28
A company that maintains a public city infrastructure was breached and information about future city projects was leaked. After the post-incident phase of the process has been completed, which of the following would be PRIMARY focus of the incident response team?

A. Restore service and eliminate the business impact.
B. Determine effective policy changes.
C. Inform the company board about the incident.
D. Contact the city police for official investigation.

Answer: B

NEW QUESTION 29
Which common source of vulnerability should be addressed to BEST mitigate against URL redirection attacks?

A. Application
B. Users
C. Network infrastructure
D. Configuration files

Answer: A

NEW QUESTION 32
Which of the following types of attackers would be MOST likely to use multiple zero-day exploits executed against high-value, well-defended targets for the purposes of espionage and sabotage?

A. Cybercriminals
B. Hacktivists

C. State-sponsored hackers
D. Cyberterrorist

Answer: C

NEW QUESTION 33
An incident at a government agency has occurred and the following actions were taken:
-Users have regained access to email accounts
-Temporary VPN services have been removed
-Host-based intrusion prevention system (HIPS) and antivirus (AV) signatures have been updated
-Temporary email servers have been decommissioned
Which of the following phases of the incident response process match the actions taken?

A. Containment
B. Post-incident
C. Recovery
D. Identification

Answer: A

NEW QUESTION 35
Which of the following characteristics of a web proxy strengthens cybersecurity? (Choose two.)

A. Increases browsing speed
B. Filters unwanted content
C. Limits direct connection to Internet
D. Caches frequently-visited websites
E. Decreases wide area network (WAN) traffic

Answer: AD

NEW QUESTION 36
As part of an organization’s regular maintenance activities, a security engineer visits the Internet Storm Center advisory page to obtain the latest list of blacklisted host/network addresses. The security engineer does this to perform which of the following activities?

A. Update the latest proxy access list
B. Monitor the organization’s network for suspicious traffic
C. Monitor the organization’s sensitive databases
D. Update access control list (ACL) rules for network devices

Answer: D

NEW QUESTION 39
Which of the following is the FIRST step taken to maintain the chain of custody in a forensic investigation?

A. Security and evaluating the electronic crime scene.
B. Transporting the evidence to the forensics lab
C. Packaging the electronic device
D. Conducting preliminary interviews

Answer: C

NEW QUESTION 41
An incident responder has collected network capture logs in a text file, separated by five or more data fields. Which of the following is the BEST command to use if the responder would like to print the file (to terminal/ screen) in numerical order?

A. cat | tac
B. more
C. sort –n
D. less

Answer: C

NEW QUESTION 46
In which of the following attack phases would an attacker use Shodan?

A. Scanning
B. Reconnaissance
C. Gaining access
D. Persistence

Answer: A

NEW QUESTION 49
When attempting to determine which system or user is generating excessive web traffic, analysis of which of the following would provide the BEST results?

A. Browser logs
B. HTTP logs
C. System logs
D. Proxy logs

Answer: D

NEW QUESTION 54
Which of the following are part of the hardening phase of the vulnerability assessment process? (Choose two.)

A. Installing patches
B. Updating configurations
C. Documenting exceptions
D. Conducting audits
E. Generating reports

Answer: AB

NEW QUESTION 55
An organization recently suffered a breach due to a human resources administrator emailing employee names and Social Security numbers to a distribution list. Which of the following tools would help mitigate this risk from recurring?

A. Data loss prevention (DLP)
B. Firewall
C. Web proxy
D. File integrity monitoring

Answer: A

NEW QUESTION 59
A cybersecurity expert assigned to be the IT manager of a middle-sized company discovers that there is little endpoint security implementation on the company's systems. Which of the following could be included in an endpoint security solution? (Choose two.)

A. Web proxy
B. Network monitoring system
C. Data loss prevention (DLP)
D. Anti-malware
E. Network Address Translation (NAT)

Answer: AB

NEW QUESTION 64
An organization recently suffered a data breach involving a server that had Transmission Control Protocol (TCP) port 1433 inadvertently exposed to the Internet. Which of the following services was vulnerable?

A. Internet Message Access Protocol (IMAP)
B. Network Basic Input/Output System (NetBIOS)
C. Database
D. Network Time Protocol (NTP)

Answer: C

NEW QUESTION 67
A security analyst has discovered that an application has failed to run. Which of the following is the tool MOST likely used by the analyst for the initial discovery?

A. syslog
B. MSConfig
C. Event Viewer
D. Process Monitor

Answer: C

NEW QUESTION 72
An incident responder discovers that the CEO logged in from their New York City office and then logged in from a location in Beijing an hour later. The incident responder suspects that the CEO's account has been compromised. Which of the following anomalies MOST likely contributed to the incident responder's suspicion?

A. Geolocation
B. False positive
C. Geovelocity
D. Advanced persistent threat (APT) activity

Answer: C

NEW QUESTION 76

Which of the following are legally compliant forensics applications that will detect an alternative data stream (ADS) or a file with an incorrect file extension? (Choose two.)

A. Disk duplicator
B. EnCase
C. dd
D. Forensic Toolkit (FTK)
E. Write blocker

Answer: BD

NEW QUESTION 79
Which of the following does the command nmap –open 10.10.10.3 do?

A. Execute a scan on a single host, returning only open ports.
B. Execute a scan on a subnet, returning detailed information on open ports.
C. Execute a scan on a subnet, returning all hosts with open ports.
D. Execute a scan on a single host, returning open services.

Answer: D

NEW QUESTION 84
While performing routing maintenance on a Windows Server, a technician notices several unapproved Windows Updates and that remote access software has been installed. The technician suspects that a malicious actor has gained access to the system. Which of the following steps in the attack process does this activity indicate?

A. Expanding access
B. Covering tracks
C. Scanning
D. Persistence

Answer: A

NEW QUESTION 86
Which of the following enables security personnel to have the BEST security incident recovery practices?

A. Crisis communication plan
B. Disaster recovery plan
C. Occupant emergency plan
D. Incident response plan

Answer: B

NEW QUESTION 91
An incident responder was asked to analyze malicious traffic. Which of the following tools would be BEST for this?

A. Hex editor
B. tcpdump
C. Wireshark
D. Snort

Answer: C

NEW QUESTION 92
A web server is under a denial of service (DoS) attack. The administrator reviews logs and creates an access control list (ACL) to stop the attack. Which of the following technologies could perform these steps automatically in the future?

A. Intrusion prevention system (IPS)
B. Intrusion detection system (IDS)
C. Blacklisting
D. Whitelisting

Answer: B

NEW QUESTION 94
When performing an investigation, a security analyst needs to extract information from text files in a Windows operating system. Which of the following commands should the security analyst use?

A. findstr
B. grep
C. awk
D. sigverif

Answer: C

NEW QUESTION 95

During which phase of a vulnerability assessment would a security consultant need to document a requirement to retain a legacy device that is no longer supported and cannot be taken offline?

A. Conducting post-assessment tasks
B. Determining scope
C. Identifying critical assets
D. Performing a vulnerability scan

Answer: C

NEW QUESTION 99

......